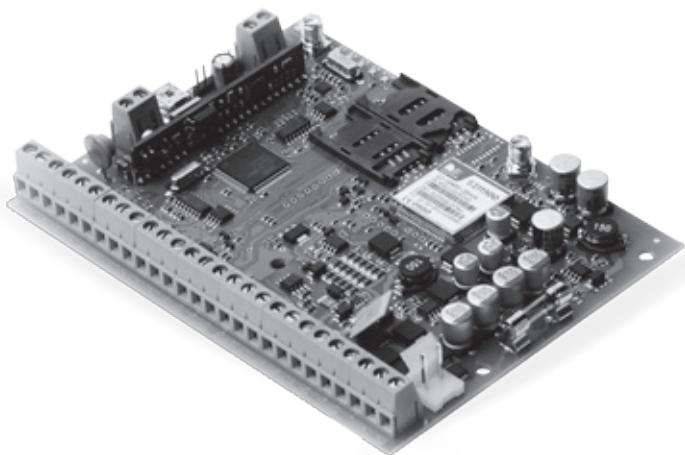


eldes



GSM ALARM AND MANAGEMENT SYSTEM

USER MANUAL **ESIM364**

COMPLIES WITH EN 50131-1 GRADE 3, CLASS II REQUIREMENTS

User Manual v1.3

Valid for ESIM364 v02.07.00 and up

Safety instructions

Please read and follow these safety guidelines in order to maintain safety of operators and people around:

- GSM alarm & management system ESIM364 (also referenced as alarm system, system or device) has radio transceiver operating in GSM 850/900/1800/1900 bands.
- DO NOT use the system where it can be interfere with other devices and cause any potential danger.
- DO NOT use the system with medical devices.
- DO NOT use the system in hazardous environment.
- DO NOT expose the system to high humidity, chemical environment or mechanical impacts.
- DO NOT attempt to personally repair the system.
- System label is on the bottom side of the device.



GSM alarm system ESIM364 is a device mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel.



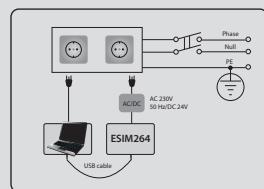
The system must be powered by main 16-24V 50 Hz ~1.5A max or 18-24V 1,5A max DC power supply which must be approved by LST EN 60950-1 standard and be easily accessible nearby the device. When connecting the power supply to the system, switching the pole terminals places does not have any affect.



Any additional devices linked to the system ESIM364 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.



Main power supply can be connected to AC mains only inside installation room with automatic 2-pole circuit breaker capable of disconnecting circuit in the event of short circuit or over-current condition. Open circuit breaker must have a gap between connections of more than 3mm and the disconnection current 5A.



Mains power and backup battery must be disconnected before any installation or tuning work starts. The system installation or maintenance must not be done during stormy conditions.



Backup battery must be connected via the connection which in the case of breaking would result in disconnection of one of battery pole terminals. Special care must be taken when connecting positive and negative battery terminals. Switching the pole terminals places is NOT allowed.



In order to avoid fire or explosion hazards the system must be used only with approved backup battery.



The device is fully turned off by disconnecting 2-pole switch off device of the main power supply and disconnecting backup battery connector.



Fuse F1 type – Slow Blown 3A. Replacement fuses have to be exactly the same as indicated by the manufacturer.



If you use I security class computer for setting the parameters it must be connected to earth.



The WEEE (Waste Electrical and Electronic Equipment) marking on this product (see left) or its documentation indicates that the product must not be disposed of together with household waste. To prevent possible harm to human health and/or the environment, the product must be disposed on in an approved and environmentally safe recycling process. For further information on how to dispose of this product correctly, contact the system supplier, or the local authority responsible for waste disposal in your area.

Limited Liability

The buyer must agree that the system will reduce the risk of fire, theft, burglary or other dangers but does not guarantee against such events.

“ELDES UAB” will not take any responsibility regarding personal or property or revenue loss while using the system. “ELDES UAB” liability according to local laws does not exceed value of the purchased system. “ELDES UAB” is not affiliated with any of the cellular providers therefore is not responsible for the quality of cellular service.

Manufacturer Warranty

The system carries a 24-month warranty by the manufacturer “ELDES UAB”. Warranty period starts from the day the system has been purchased by the end user. The warranty is valid only if the system has been used as intended, following all guidelines listed in the manual and within specified operating conditions. Receipt must be kept as a proof of purchase date.

The warranty is voided if the system has been exposed to mechanical impact, chemicals, high humidity, fluids, corrosive and hazardous environments or other force majeure factors.

Technical Support

If you require more detailed information on your system or in case of system failure occurrence, please, contact your alarm system installer.

About User Manual

This document describes basic configuration and usage of alarm system ESIM364. It is very important to read the user manual before starting to use the system.

Package Content

1. ESIM364.....	qty. 1
2. Microphone.....	qty.1
3. SMA antenna.....	qty. 2
4. Buzzer.....	qty. 1
5. Back-up battery connection wire.....	qty. 1
6. User manual.....	qty. 1
7. Resistors 5,6kΩ.....	qty.12
8. Resistors 3,3kΩ.....	qty. 6
9. Plastic standoffs.....	qty. 4

NOTE: For complete system configuration and control, please refer to ESIM364 installation manual located at www.eldes.lt/en/download

CONTENTS

1. GENERAL INFORMATION	6
1.1 Short Description of Main Definitions.....	6
1.2 EKB2 Keypad Overview.....	7
1.3 EKB3/EKB3W Keypad Overview.....	9
1.4 Partitions.....	9
2. TECHNICAL SPECIFICATIONS	10
2.1 Electrical & Mechanical Characteristics.....	10
2.2 Main Unit, LED & Connector Functionality.....	11
2.3 Wiring Diagrams.....	12
2.3.1 General Wiring.....	12
2.3.2 Zone Connection Types	12
3. BASIC CONFIGURATION & USE	13
3.1 Setting Up Date & Time	13
3.2. Arming, Disarming the System & Turning Off the Alarm.....	14
3.2.1 Arm, Disarm & Turn off the Alarm by Phone Call	14
3.2.2 Arm by SMS text message	15
3.2.3 Disarm & Turn off the Alarm by SMS text message	15
3.2.4 Arm by EKB2 Keypad.....	16
3.2.5 Disarm and Turn off the Alarm by EKB2 Keypad	18
3.2.6 Arm by EKB3 Keypad	19
3.2.7 Disarm and Turn off the Alarm by EKB3 Keypad	20
3.2.8 Arm by EKB3W Keypad	21
3.2.9 Disarm and Turn off the Alarm by EKB3W Keypad	22
3.2.10 Arm by iButton® Key	23
3.2.11 Disarm & Turn off the Alarm by iButton® Key	23
3.2.12 Arm by EWK1 – Wireless Key-fob.....	24
3.2.13 Disarm & Turn off the Alarm by EWK1 – Wireless Key-fob.....	25
3.2.14 Arm by EWK2 – Wireless Key-fob.....	26
3.2.15 Disarm & Turn off the Alarm by EWK2 – Wireless Key-fob	27
3.3 Arming in STAY Mode.....	28
3.3.1 Arm by EKB2 Keypad in STAY Mode.....	29
3.4 Alarm Indications & Viewing Violated Zones / Tamper.....	32
3.5 Bypassing & Activating Zones	34
3.6 Viewing System Information.....	35
3.7 Managing Periodical System Information.....	35
3.8 Viewing Zone & PGM Output Information.....	36
3.9 Managing Temperature Information	37
3.10 Indication of System Faults	38
3.11 Controlling Electrical Appliances.....	40
3.12 Turning ON/OFF the Electrical Appliances for a Determined Time Period	41
3.13 Viewing Event and Alarm Logs	42
4. IF THE ALARM SYSTEM IS CONNECTED TO MONITORING STATION.....	43

Copyright © "ELDES UAB", 2014. All rights reserved

It is not allowed to copy and distribute information in this document or pass to a third party without advanced written authorization by "ELDES UAB". "ELDES UAB" reserves the right to update or modify this document and/or related products without a warning. Hereby, "ELDES UAB" declares that this GSM alarm and management system ESIM364 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at www.eldes.lt



Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

15.105 statement (for digital devices)

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be located or operating in conjunction with any other antenna or transmitter.



1. GENERAL INFORMATION

ESIM364 is an alarm system for private houses, cottages, village houses, garages, warehouses and other buildings, also capable of turning on/off the electrical appliances by SMS text message and alarm system keypad. This alarm system provides a simple thus effective way of use.

The system may consist of:

- ESIM364 alarm system device.
- Up to 4 EKB2/EKB3 wired keypads.
- Up to 4 EKB3W wireless keypads.
- Wired and/or wireless detection devices: movement sensors, magnetic door contacts, smoke sensors etc.
- Other devices: indoor/outdoor sirens, zone/PGM output expansion modules, heating, lighting, gates etc.

For more details on ESIM364 system, please, consult with your alarm system installer.

1.1 Short Description of Main Definitions

The following table provides the explanation of main definitions which are met in this user manual.

Definition	Description
System; alarm system	ESIM364 device
SMS	Short Message Service text
Keypad	Device with a set keys allowing to configure & control the system, view violated zones & system faults
EKB2	Model of wired LCD keypad
EKB3	Model of wired LED keypad
EKB3W	Model of wireless LED keypad
EWK1	Model of wireless keyfob
EWK2	Model of wireless keyfob
User phone number; User 1... 10	Phone number of the user allowed to control and receive SMS text messages from the system
System phone number	Phone number of the SIM card inserted in ESIM364 device
User password	4-digit combination intended for system arming/disarming using a keypad
iButton® key	Microchip containing a unique 64-bit ID code intended for system arming/disarming
Zone	Alarm system input for wired and wireless sensor connection
PGM output	Alarm system output for connection of electrical appliances (heating, lighting, gates etc.)
Partition	Section dividing one alarm system into two or more independent parts software-wise

1.2 EKB2 Keypad Overview

EKB2 is an LCD keypad intended for using with ESIM364 alarm system.

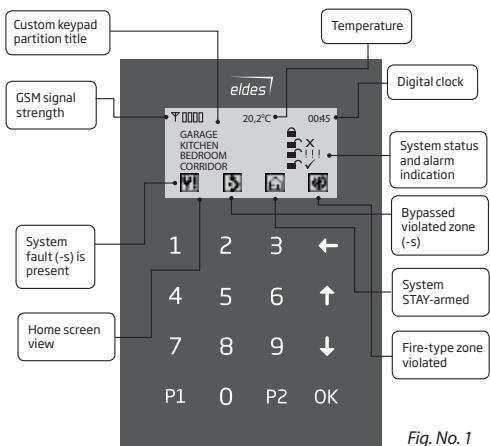


Fig. No. 1

Keys Functionality

	One menu level back / cancel
	Menu navigation – up
	Menu navigation – down
	Confirm (enter) value
	Value typing
	Minus character to enter negative temp. value
	Additional menu / minus character to enter negative temp. value

Main Messages & Icons

Icon	Description
	Partition is armed and menu is locked (by default - disabled)
	Partition is disarmed and menu is unlocked (by default - disabled)
	Configuration mode activated
	Zone or tamper alarm in partition
	Partition is ready to be armed.
	Partition is not ready to be armed – one or more zones / tampers violated.
	One or more system faults present
	One or more violated zones bypassed
	One or more partitions STAY-armed
	One or more Fire-type zones violated
	Alarms in alarm log present

EKB2 LCD screen is intended for displaying alarm system status messages and alerts. Icon  is displayed on the screen that no zones and/or tampers are violated and the partition is prepared for arming. Icon  shows up in case of zone violation or icon  if system faults are present. The partition cannot be armed until the violated zone (-s) is restored, disabled, bypassed or set up to operate under Force mode or violated tamper (-s) is restored. By default, the following faults allow partition arming if present:

- main power supply is lost.
- low battery.
- battery dead or missing.
- battery failed.
- siren failed.
- date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.
- Keypad lost.

Audio Indication

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the buzzer emits short beeps in case of alarm.

Visual Indication

EKB2 can be used even in dark premises as the LCD screen and keys are illuminated continuously. The illumination level lowers down if 3 minutes after the last key-touch expires while the system is disarmed. In case of alarm, the keypad illumination level is boosted and stays in this state until the system is disarmed.

1.3 EKB3/EKB3W Keypad Overview

EKB3/EKB3W is a LED keypad intended for using with ESIM364 alarm system.

LED Functionality

ARMED	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - system is ready - no violated zones and tampers
SYSTEM	Steady ON - system faults; flashing - violated high-numbered zones
BYP5	Steady ON - zone bypass mode
1-12	Steady ON - violated zone

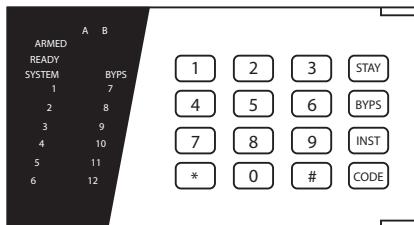


Fig. No. 2

Keys Functionality

[BYP5]	Bypass violated zone
[CODE]	System fault list / violated high-numbered zone indication / violated tamper indication
[*]	Clear typed in characters
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[1] ... [4]	Keypad partition switch (only on EKB3) / steady ON - armed partition indication (only on EKB3) / flashing - violated partition indication (only on EKB3)
[1] ... [2]	Keypad partition switch (only on EKB3W)
[0]	Simultaneous 4-partition arming (only on EKB3)
[STAY]	Manual system arming in Stay mode
[INST]	1st character for Configuration mode activation/deactivation command

The green indicator **READY** indicates that no zones and/or tampers are violated and the system is prepared for arming. Yellow indicator **SYSTEM** lights up or flashes in case of zone violation or if system faults are present. The partition cannot be armed until the violated zone (-s) is restored, disabled, bypassed or set up to operate under Force mode or violated tamper (-s) is restored. By default, the following faults allow partition arming if present:

- main power supply is lost.
- low battery.
- battery dead or missing.
- battery failed.
- siren failed.
- date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.
- Keypad lost.

Audio Indication

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the buzzer emits short beeps in case of alarm.

Visual Indication

EKB3 keys have a LED back-light, therefore it is possible to use this keypad even in dark premises. The back-light lasts for 3 minutes after the last key-stroke while the system is disarmed. In case of alarm, the keypad back-light turns ON and lasts until the system is disarmed.

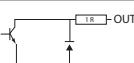
EKB3W keys have a LED back-light, which will be activated once any key is pressed. Due to battery power saving reasons, the back-light and LED light last for 10 seconds after the last key-stroke.

1.4 Partitions

Your alarm system may be divided into up to 4 partitions: Partition 1 - Partition 4. Each system partition operates independently from each other, therefore dividing the system into partitions allows to use 1 alarm system unit to secure up to 4 different areas, for example: office and warehouse, house and garage etc. By default configuration, the system is NOT divided into partitions and all user phone numbers, user passwords, keypads, iButton® keys, zones are assigned to Partition 1.

2. TECHNICAL SPECIFICATIONS

2.1 Electrical & Mechanical Characteristics

Electrical & Mechanical Characteristics	
Main power supply	16-24V 50 Hz ~1.5A max / 18-24V —— 1,5A max
Current in standby without external sensors and keypad	Up to 80mA
Recommended backup battery voltage, capacity	12V, 1,3-7 Ah
Recommended backup battery type	Lead-Acid
Backup battery charge current	up to 500mA
Backup battery charge duration	up to 30 hours for 7Ah battery
GSM modem frequency	850/900/1800/1900MHz
Cable type for GSM/GPRS antenna connection	Shielded
Number of zones on-board	6 (ATZ mode: 12)
Nominal zone resistance	5,6kΩ (ATZ Mode: 5,6kΩ and 3,3kΩ)
Number of PGM outputs on-board	4
On-board PGM output circuit	 <p>Open Collector Output. Output is pulled to COM when turned ON.</p>
Maximum commuting on-board PGM output values	4 x Voltage – 30V; current – 500mA.
BELL: Siren output when activated	Connected to COM
BELL: Maximum siren output current	1A
BELL: Maximum cable length for siren connection	Up to 100 meters
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
AUX: Maximum accumulative current of auxiliary equipment	1,1A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100 meters
AUX: Cable type for auxiliary equipment connection	Unshielded
BUZ: Maximum current of mini buzzer	150mA
BUZ: Power supply voltage of buzzer	5V DC
BUZ: Cable type for mini buzzer connection	Unshielded
Supported temperature sensor model	Maxim®/Dallas® DS18S20, DS18B20
Maximum supported number of temperature sensors	8
DATA: Maximum cable length for 1-Wire communication	Up to 30 meters
DATA: Cable type for 1-Wire communication	Unshielded
Supported ibutton key model	Maxim®/Dallas® DS1990A
Maximum supported number of iButton keys	16
Maximum supported number of keypads	4 x EKB2 / EKB3
Y/G: Maximum cable length for RS485 communication	Up to 100 meters
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2 meters
MIC: Cable type for microphone connection	Unshielded
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless communication range	Up to 30m in premises; up to 150m in open areas
Maximum supported number of wireless devices	32
Event log size	500 events
Maximum supported number of zones	76
Maximum supported number of PGM outputs	76
Cable type for zone and PGM output connection	Unshielded
Communications	SMS, Voice calls, GPRS network, RS485, CSD, PSTN, Ethernet via ELAN3-ALARM
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS, SIA IP
Dimensions	140x100x1 w8mm
Operating temperature range	-20...+55 °C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)

2.2 Main Unit, LED & Connector Functionality

Main Unit Functionality

GSM MODEM	GSM network 850/900/1800/1900MHz modem
SIM CARD1	Primary SIM card slot / holder
SIM CARD2	Secondary SIM card slot / holder
DEF	Pins for restoring default settings
USB	Mini USB port
FUSE F1	3A fuse
W-LESS ANT	Wireless antenna SMA type connector
GSM/GPRS ANT	GSM/GPRS antenna SMA type connector
MODULES*	Slots for EA1, EA2 or EPGM8 module

LED Functionality

NETW	GSM network signal strength
C1	PGM output C1 status - on/off
C2	PGM output C2 status - on/off
C3	PGM output C3 status - on/off
C4	PGM output C4 status - on/off
STAT	Micro-controller status

Connector Functionality

TIP*	PSTN (landline) terminal
RING*	PSTN (landline) terminal
DATA	1-Wire® interface for iButton key & temperature sensor connection
+5V	Temperature sensor power supply terminal (+5V)
MIC-	Microphone negative terminal
MIC+	Microphone positive terminal
BUZ-	Buzzer negative terminal
BUZ+	Buzzer positive terminal
C1 - C4	PGM output terminals
Z1 - Z6	Security zone terminals
Y	RS485 interface for communication (yellow wire)
G	RS485 interface for communication (yellow wire)
COM	Common return terminal
BELL-	Siren negative terminal
BELL+	Siren positive terminal
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
AC/DC	Main power supply terminals
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

* - Optional, implementable on request in advance

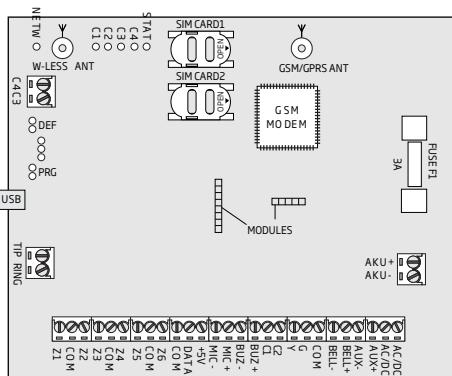


Fig. No.3

2.3 Wiring Diagrams

2.3.1 General Wiring

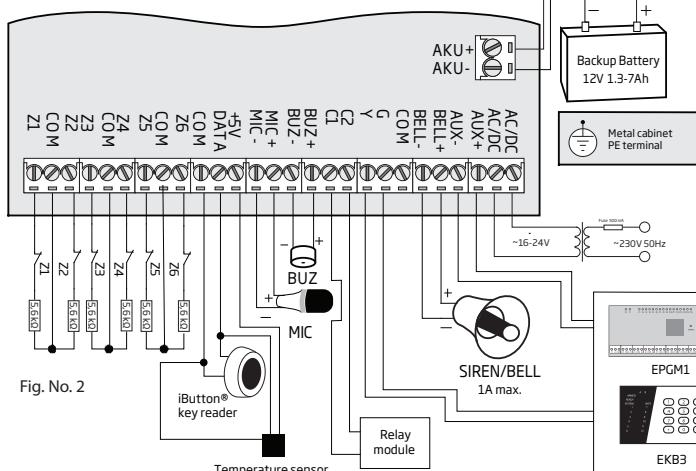


Fig. No. 2

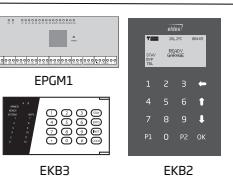


Fig. No. 4

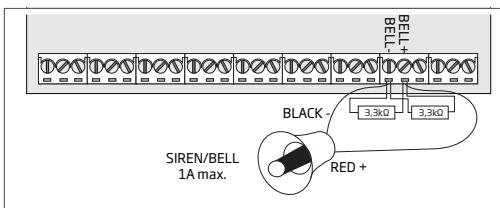


Fig. No. 5

Siren status monitoring

By default, the system monitors siren status and indicates system fault on the keypad if the siren is broken/disconnected. However, this feature requires a pair of parallelly connected resistors of 3,3kΩ nominal across **BELL+** and **BELL-** terminals.

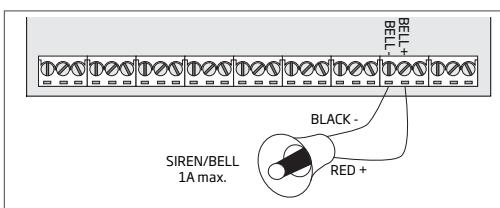


Fig. No. 6

No siren status monitoring

If the siren status monitoring feature is not required, do not connect any resistor in parallel and disable siren fault indication on the keypad (see **3.10 Indication of System Faults**).

2.3.2 Zone Connection Types

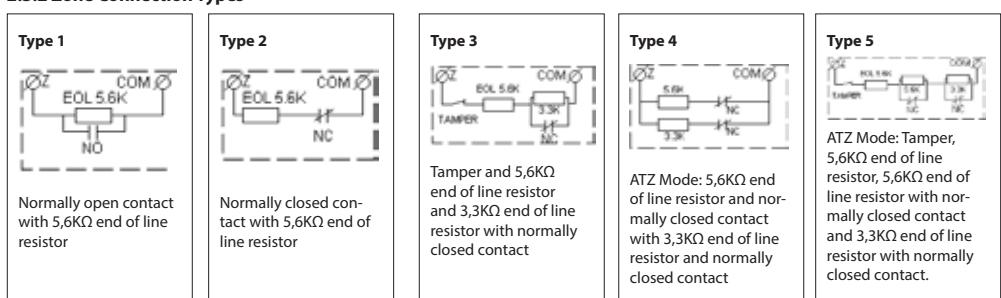


Fig. No. 7

3. BASIC CONFIGURATION & USE

ATTENTION: System configuration described in this chapter is based on default system parameter values. Your alarm system installer may have changed those values. For more details, please, contact your alarm system installer.

This chapter provides a description of basic configuration and use of ESIM364 alarm system by the following methods:

- SMS text message.
- Phone call.
- EKB2 keypad.
- EKB3 keypad.
- EKB3W wireless keypad.
- iButton® key.
- EWK1 wireless keyfob.
- EWK2 wireless keyfob

SMS

In order to configure and control the system using SMS text message, send the text command to the ESIM364 system phone number from one of the preset user phone numbers. In this user manual the underscore symbol " _ " represents one space character. Every underscore symbol must be replaced by a single space character. There must be no spaces or other unnecessary characters at the beginning and at the end of the message. **ssss** – 4-digit SMS password set by your alarm system installer.

EKB2

The system configuration and control by EKB2 keypad is performed by navigating throughout the menu section list displayed on LCD screen. To navigate in the menu path, touch \downarrow , \uparrow keys to select the desired menu section and touch *OK* key for value confirmation or cancel/ go one menu section back by touching \leftarrow key. The value can be typed in directly by touching $0\dots 9$ keys while highlighting the desired menu section. EKB2 menu type is "circle", therefore when the last section in the menu list is selected, you will be brought back to the beginning of the list after touching the \downarrow key. In this user manual, the menu path is provided under "tree" view by starting at home screen view. In this user manual valid parameter range is indicated in brackets..

**EKB3/
EKB3W**

The system configuration and control by EKB3/EKB3W keypad is carried out by entering a valid configuration command using the number keys $0\dots 9$, $[#]$ key for confirmation and $[*]$ key to cancel the characters that are being entered. Alternatively, the user can wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the entered characters have been cancelled. When typing in the characters, the indication of each pressed key is provided by short beep of keypad buzzer. Additionally, the red indicators light up when the number keys $0\dots 9$ are being pressed. Some commands require *[BYP5]*, *[CODE]* and *[STAY]* keys as well. The structure of a standard configuration command is a combination of digits. The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

NOTE: If you have accidentally typed in an unnecessary character (-s), please press $[*]$ key or wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the typed in characters have been cleared.

3.1 Setting Up Date & Time

NOTE: When the alarm system is connected to a monitoring station the date and time are set automatically. The system retrieves this data from the monitoring station by itself.

SMS

1. Send the following SMS text message to the phone number of ESIM364 alarm system:

SMS text message content:

ssss_yyyy.mm.dd_hr:mm

Value: yyyy – year; mm – month, range – [01... 12]; dd – day, range - [01... 31]; hr – hours, range – [00... 23], mn – minutes, range – [00... 59].

Example: 1111_2011.12.15_13:45

2. The system will reply with confirmation by SMS text message to user phone number who sent the SMS text message after the date & time is set successfully.

Navigate through the following menu path using **OK** and arrow keys and enter the date and time values using the number keys:

Menu path:

OK → **uuuu** → **OK** → **DATE/TIME SETTINGS** → **OK** → **yyyy-mm-dd_hr:mn** → **OK**

Value: **uuuu** – 4-digit user or master code; **yyyy** – year; **mm** – month, range – [01... 12]; **dd** – day, range - [01... 31]; **hr** – hours, range – [00... 23], **mn** – minutes, range – [00... 59].

Example: 2011-12-15 13:45

3.2. Arming, Disarming the System & Turning Off the Alarm

Before arming the system it is necessary to close all doors and windows in the secured area and move yourself away from the movement detection field.

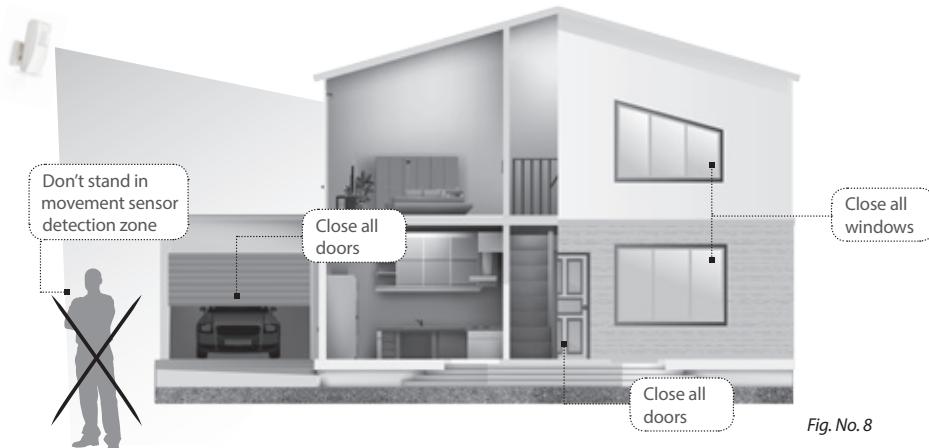


Fig. No. 8

3.2.1 Arm, Disarm & Turn off the Alarm by Phone Call

ATTENTION: User must leave the secured area before arming the system by phone call.



1. To arm, disarm the system & turn off the alarm, make a phone call to the system's phone number from any of 10 available user phone numbers. The phone call is free charge as the system rejects it and carries out arming/disarming procedure after-wards. When arming – the system rejects the phone call after 2 rings, when disarming – the system rejects the phone call immediately.
2. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by long steady beep emitted by buzzer connected to the alarm system (if any).
3. When the system is successfully armed or disarmed, it will reply with confirmation by SMS text message to the user phone number that made a phone call.



Fig. No. 9

4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it and it will reply with violated zone / tamper number to the user phone number that made a phone call. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing & Activating Zones**.

3.2.2 Arm by SMS text message



1. Leave the secured area.
2. To arm the system, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:
SMS text message content:
`ssss_ARMp` or `ssss_ARMp,p,p,p`
Value: *p* - partition number, range - [1... 4]
Example: `1111_ARM1`
3. When the system is successfully armed, it will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.



Fig. No. 10

4. When attempting to arm the system in case of violated zone / tamper presence, the system not permit to arm it and it will reply with violated zone / tamper number to the user phone number that sent the SMS text message. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing & Activating Zones**.

3.2.3 Disarm & Turn off the Alarm by SMS text message



1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by long steady beep emitted by buzzer connected to the alarm system (if any).
2. To disarm the system or turn off the alarm, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:
SMS text message content:
`ssss_DISARMp` or `ssss_DISARMp,p,p,p`
Value: *p* - partition number, range - [1... 4]
Example: `1111_DISARM1,3,4`
3. When the system is successfully disarmed, it will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.

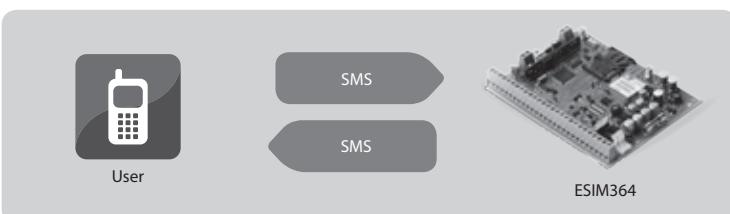


Fig. No. 11

3.2.4 Arm by EKB2 Keypad



1. To arm the system, enter any out of 29 available 4-digit user codes or master code using the number keys:



Fig. No. 12

Enter user/master code (and select partition):

Non-partitioned system:

a) $uuuu \rightarrow OK$

b) $OK \rightarrow uuuu \rightarrow OK \rightarrow ARM/DIS PARTITION \rightarrow OK \rightarrow [p] \text{ part-name} \rightarrow OK$

Partitioned system – arming a single partition:

$uuuu \rightarrow OK \rightarrow [p] \text{ part-name} \rightarrow OK$ or $OK \rightarrow uuuu \rightarrow OK \rightarrow ARM/DIS PARTITION \rightarrow OK \rightarrow [p] \text{ part-name} \rightarrow OK$

Partitioned system – arming multiple partitions:

$uuuu \rightarrow OK \rightarrow ARM \text{ ALL} \rightarrow OK$ or $OK \rightarrow uuuu \rightarrow OK \rightarrow ARM/DIS PARTITION \rightarrow OK \rightarrow ARM \text{ ALL} \rightarrow OK$

Value: $uuuu$ – 4-digit user or master code; p – partition number, range – [1... 4],
 part-name – up to 15 characters partition name.

Example: 2222 → OK → [2] PART2 → OK

Non-partitioned system:

- a) When a valid user or master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps, the keypad will switch to home screen view and display the countdown timer.
- b) When a valid user or master code is entered, the keypad will display the partition selection menu. Once the partition is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. If **←** key is touched during exit delay, the keypad will return to home screen view and display the countdown timer next to the partition name .

When the system is successfully armed:

- by default, the countdown timer will disappear.
- If enabled, the keypad will display icon next to the partition name that has been armed.

Partitioned system; arming a single partition as the keypad is assigned to – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. If **←** key is touched during exit delay, the keypad will return to home screen view and display the countdown timer next to the partition name that is being armed. When successfully armed:

- by default, the countdown timer will disappear.
- if enabled, the keypad will display icon next to the partition name that has been armed.

Partitioned system; arming a different single partition than the keypad is assigned to – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay, but will not indicate it on EKB2 keypad due to the difference between keypad partition and the one being armed. Then the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow.

Alternatively, the  key may be touched in order to instantly return to home screen view.

Partitioned system; arming multiple partitions simultaneously – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **ARM ALL** menu item is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display multiple **ARMING part-name** messages for 3 seconds reflecting each partition the user/master code is assigned to, followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. If key  is touched during exit delay, the keypad will return to home screen view and display the countdown timers next to the partition names the keypad is assigned to. When successfully armed:

- by default, the countdown timers will disappear.
- If enabled, the keypad will display  icon next to the partition name that has been armed.

3. In addition, when the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.
4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it. For more details on how to view the violated zone / tamper number, please refer to **3.4 Alarm Indications and Viewing Violated Zones / Tamers**. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing and Activating Zones**.

NOTE: If the user fails to enter a correct user/master code 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user/master code. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

NOTE: The keypad will display  icon next to the armed partition name in home screen view only if **Show ARMED status in keypad** parameter is enabled and the keypad is assigned to the same partition (-s) as the armed one.

3.2.5 Disarm and Turn off the Alarm by EKB2 Keypad

EKB2

1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by short beeps emitted by keypad buzzer and by long steady beep emitted by buzzer connected to the alarm system (if any).
2. To disarm the system or turn off the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys:



Fig. No. 13

Enter user/master code (and select partition):

Non-partitioned system:

- a) **uuuu → OK**
- b) **OK → uuuu → OK → ARM/DIS PARTITION → OK → [p] part-name → OK**

Partitioned system – disarming a single partition: **uuuu → OK → [p] part-name → OK or OK → uuuu → OK → ARM/DIS PARTITION → OK → [p] part-name → OK**

Partitioned system – disarming multiple partitions: **uuuu → OK → ARM ALL → OK or OK → uuuu → OK → ARM/DIS PARTITION → OK → ARM ALL → OK**

Value: *uuuu* – 4-digit user or master code; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.

Example: **2222 → OK → [2] PART2 → OK**

3. When the system is successfully disarmed:

Non-partitioned system:

- a) When a valid user or master code is entered, the keypad will switch to home screen view. If enabled,  icon will be displayed next to the partition name in home screen view.
- b) When a valid user or master code is entered, the keypad will display the partition selection menu. Once the partition is selected, the keypad will display **part-name DISARMED** message for 3 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the  key may be touched in order to instantly return to home screen view. If enabled,  icon will be displayed next to the partition name in home screen view.

Partitioned system; disarming a single partition – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be disarmed is selected, the keypad will display **part-name DISARMED** message for 3 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the  key may be touched in order to instantly return to home screen view. If enabled, in home screen view  icon will be displayed next to the partition name that has been disarmed.

Partitioned system; disarming multiple partitions simultaneously – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **DISARM ALL** menu item is selected, the keypad will display multiple **part-name DISARMED** messages for 3 seconds reflecting each partition the user/master code is assigned to and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the  key may be touched in order to instantly return to home screen view. If enabled, in home screen view  icon will be displayed next to the partition name that has been disarmed.

4. In addition, when the system is successfully disarmed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.

NOTE: If the user fails to enter a correct user password 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user password. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

NOTE: The keypad will display  icon next to the disarmed partition name in home screen view only if **Show ARMED status in keypad** parameter is enabled and the keypad is assigned to the same partition (-s) as the disarmed one.

3.2.6 Arm by EKB3 Keypad

EKB3

ATTENTION: The following procedure is described based on 4-partition mode operation on EKB3 keypad. If your alarm system installer has enabled 2-partition mode, the arming procedure using EKB3 keypad will be carried out identically to EKB3W wireless keypad. For more details on 2-partition mode, please refer to **3.2.8. Arm by EKB3W Keypad.**

1. a) To arm a system partition that the keypad is assigned to, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: *uuuu* – 4-digit user or master code

Example: 2222

1. b) To arm a different system partition, switch the keypad partition by pressing and holding the [1]... [4] key for 3 seconds until you will hear 3 short beeps:

Switch keypad partition:

Hold the [1]... [4] key and release it after 3 short beeps:

Value: [1]... [4] key – partition number 1... 4

After switching the keypad partition, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: *uuuu* – 4-digit user or master code

Example: 2222

1. c) To arm multiple partitions simultaneously, press and hold the [0] key until you will hear 3 short beeps. Then enter any out of 29 available 4-digit user codes or master code using the number keys:

Hold the [0] key, release it after 3 short beeps and enter user/master code:

0 uuuu

Value: *uuuu* – 4-digit user or master code.

Example: 0 2222

2. The keypad indicator ARMED and [1]... [4] key, corresponding the partition number that is being armed, will light ON and the system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area. The countdown is indicated by short beeps emitted by keypad buzzer and the buzzer connected to the alarm system (if any).
3. When the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.



Fig. No. 14

4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it. For more details on how to view the violated zone / tamper number, please refer to **3.4 Alarm Indications and Viewing Violated Zones / Tampers**. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing and Activating Zones**.

ATTENTION: Your alarm system installer must enable keypad partition switch feature before you can use it.

3.2.7 Disarm and Turn off the Alarm by EKB3 Keypad

EKB3

ATTENTION: The following procedure is described based on 4-partition mode operation on EKB3 keypad. If your alarm system installer has enabled 2-partition mode, the disarming procedure using EKB3 keypad will be carried out identically to EKB3W wireless keypad. For more details on 2-partition mode, please refer to [3.2.9. Disarm by EKB3W Keypad](#).

1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by short beeps emitted by keypad buzzer and long steady beep emitted by buzzer connected to the alarm system (if any).
2. a) To disarm a system partition that the keypad is assigned to, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: uuuu – 4-digit user or master code

Example: 2222

- b) To disarm a different system partition, switch the keypad partition by pressing and holding the [1]... [4] key for 3 seconds until you will hear 3 short beeps:

Switch keypad partition:

Hold the [1]... [4] key and release it after 3 short beeps:

Value: [1]... [4] key – partition number 1... 4

After switching the keypad partition, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: uuuu – 4-digit user or master code

Example: 2222

- c) To disarm multiple partitions simultaneously, press and hold the [0] key until you will hear 3 short beeps. Then enter any out of 29 available 4-digit user codes or master code using the number keys:

Hold the [0] key, release it after 3 short beeps and enter user/master code:

0 uuuu

Value: uuuu – 4-digit user or master code.

Example: 0 2222

3. When the system is successfully disarmed, the keypad indicator ARMED and [1]... [4] key, corresponding the partition number that has been disarmed, will light OFF and the system will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.

ATTENTION: Your alarm system installer must enable keypad partition switch feature before you can use it..

3.2.8 Arm by EKB3W Keypad



- a) To arm the system partition that the keypad is assigned to, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: uuuu – 4-digit user or master code

Example: 2222

- b) To arm a different system partition, switch the keypad partition by pressing and holding the [1]... [2] key for 3 seconds until you will hear 3 short beeps:

Switch keypad partition:

Hold the [1]... [2] key and release it after 3 short beeps:

Value: [1]... [2] key – partition number 1... 2

After switching the keypad partition, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: uuuu – 4-digit user or master code

Example: 2222

2. The keypad indicator **ARMED** will light ON and the system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area. The countdown is indicated by short beeps emitted by keypad buzzer and the buzzer connected to the alarm system (if any).
3. When the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.
4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it. For more details on how to view the violated zone / tamper number, please refer to **3.4 Alarm Indications and Viewing Violated Zones / Tampers**. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing and Activating Zones**.

ATTENTION: Your alarm system installer must enable keypad partition switch feature before you can use it..

NOTE: The user can control only the first two system partitions using EKB3W keypad.

3.2.9 Disarm and Turn off the Alarm by EKB3W Keypad



1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by short beeps emitted by keypad buzzer and long steady beep emitted by buzzer connected to the alarm system (if any).
2. a) To disarm the system partition that the keypad is assigned to, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: *uuuu* – 4-digit user or master code

Example: 2222

- b) To disarm a different system partition, switch the keypad partition by pressing and holding the [1]... [2] key for 3 seconds until you will hear 3 short beeps:

Switch keypad partition:

Hold the [1]... [2] key and release it after 3 short beeps:

Value: [1]... [2] key – partition number 1... 2

After switching the keypad partition, enter any out of 29 available 4-digit user codes or master code using the number keys:

Enter user/master code:

uuuu

Value: *uuuu* – 4-digit user or master code

Example: 2222

3. When the system is successfully disarmed, the keypad indicator **ARMED** will light OFF and the system will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.

ATTENTION: Your alarm system installer must enable keypad partition switch feature before you can use it..

NOTE: The user can control only the first two system partitions using EKB3W keypad.

3.2.10 Arm by iButton® Key

1. To arm the system, touch the iButton® key reader by any out of 5 iButton® keys:



Fig. No. 15

2. The system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area. The countdown is indicated by short beeps emitted by buzzer connected to the alarm system (if any).
3. When the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the iButton key.



4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it and it will reply with violated zone / tamper number to the user phone number that made a phone call. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing & Activating Zones**.

3.2.11 Disarm & Turn off the Alarm by iButton® Key

1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by long steady beep emitted by buzzer connected to the alarm system (if any).
2. To disarm the system or turn off the alarm, touch the iButton® key reader by any out of 5 iButton® keys:

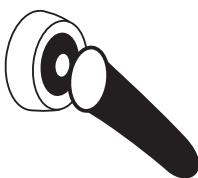


Fig. No. 17

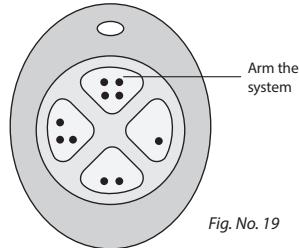
3. When the system is successfully disarmed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the iButton key.



3.2.12 Arm by EWK1 – Wireless Key-fob

EWK1

1. To arm the system, press 1 out of 4 EWK1 buttons (by default –  button) assigned to arm the alarm system.



2. The system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area. The countdown is indicated by short beeps emitted by buzzer connected to the alarm system (if any).
3. When the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the keyfob.



4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it and it will reply with violated zone / tamper number to the user phone number that made a phone call. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing & Activating Zones**

3.2.13 Disarm & Turn off the Alarm by EWK1 – Wireless Key-fob

EWK1

1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by long steady beep emitted by buzzer connected to the alarm system (if any).
2. To disarm the system or turn off the alarm, press 1 out of 4 EWK1 buttons (by default –  button) assigned to disarm the alarm system

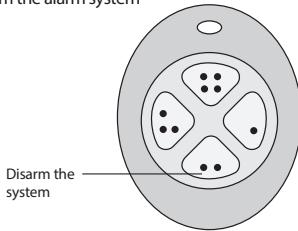


Fig. No. 21

3. When the system is successfully disarmed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the keyfob.

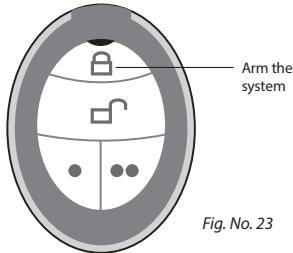


Fig. No. 22

3.2.14 Arm by EWK2 – Wireless Key-fob

EWK2

1. To arm the system, press 1 out of 4 EWK2 buttons (by default –  button) assigned to arm the alarm system.



2. The system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area. The countdown is indicated by short beeps emitted by buzzer connected to the alarm system (if any).
3. When the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the keyfob.



4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it and it will reply with violated zone / tamper number to the user phone number that made a phone call. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing & Activating Zones**

3.2.15 Disarm & Turn off the Alarm by EWK2 – Wireless Key-fob

EWK2

1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused. The countdown is indicated by long steady beep emitted by buzzer connected to the alarm system (if any).
2. To disarm the system or turn off the alarm, press 1 out of 4 EWK2 buttons (by default –  button) assigned to disarm the alarm system

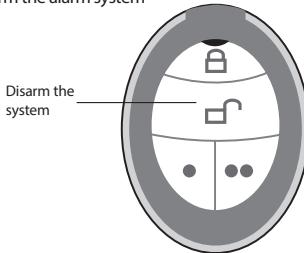


Fig. No. 25

3. When the system is successfully disarmed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the keyfob.



Fig. No. 26

3.3 Arming in STAY Mode

EKB2

**EKB3/
EKB3W**



EWK1

EWK2

Stay mode allows the user to arm and disarm the alarm system without leaving the secured area. If the zones with Stay attribute enabled are violated when the system is Stay armed, no alarm will be caused. Typically, this feature is used when arming the system at home before going to bed.

The system can be Stay-armed under the following conditions:

- If a zone with Stay attribute enabled is NOT violated during exit delay, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must be used that provide exit delay i. e. EKB2/EKB3 - wired keypad, EKB3W - wireless keypad, iButton key, EWK1/EWK2 - wireless keyfob,
- The system will instantly arm in Stay mode when using EKB2/EKB3/EKB3W keypad. For more details, please refer to **3.3.1 Arm by EKB2 Keypad in STAY Mode**, **3.3.2 Arm by EKB3 Keypad in STAY Mode** and **3.3.3 Arm by EKB3W Wireless Keypad in STAY Mode** respectively.

NOTE: *Delay Zone Becomes Instant in Stay Mode* feature may be enabled on your system. In that case the alarm will be caused instantly instead of entry delay countdown being initiated if a delay zone becomes violated while the system is operating in Stay mode. For more details, please, contact your alarm system installer.

3.3.1 Arm by EKB2 Keypad in STAY Mode

EKB2

1. To arm the system in Stay mode, navigate through the following menu path using P2 and arrow keys and enter a valid user or master code using the number keys:

Enter user/master code (and select partition):

Non-partitioned system: P2 → uuuu → OK

Partitioned system – arming a single partition: P2 → uuuu → OK → [p] part-name → OK

Partitioned system – arming multiple partitions: P2 → uuuu → OK → ARM ALL → OK

Value: uuuu – 4-digit user or master code; p – partition number, range – [1... 4], part-name – up to 15 characters partition name.

Example: P2 → 2222 → OK → [2] PART2 → OK

Non-partitioned system:

When a valid user or master code is entered, the system will switch to home screen view and display  icon. In addition, if enabled, the keypad will display  icon next to the partition name that has been Stay-armed.

Partitioned system; arming a single partition as the keypad is assigned to – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the keypad will display **part-name ARMED** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the keypad will return to home screen view and display  icon. Alternatively, the  key may be touched in order to instantly return to home screen view. In addition, if enabled, the keypad will display  icon next to the partition name that has been Stay-armed.

Partitioned system; arming a different single partition than the keypad is assigned to – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the keypad will display **part-name ARMED** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the keypad will return to home screen view. Alternatively, the  key may be touched in order to instantly return to home screen view.

Partitioned system; arming multiple partitions simultaneously – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **ARM ALL** menu item is selected, the keypad will display multiple **part-name ARMED** messages for 3 seconds reflecting each partition the user/master code is assigned to, followed by partition selection menu. When the keypad back-light timeout expires, the keypad will return to home screen view and display  icon. Alternatively, the  key may be touched in order to instantly return to home screen view. In addition, if enabled, the keypad will display  icon next to the partition name the keypad is assigned to and the partition (-s) that has (-ve) been Stay-armed.

3. In addition, when the system is successfully armed, it will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.
4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it. For more details on how to view the violated zone / tamper number, please refer to **3.4 Alarm Indications and Viewing Violated Zones / Tamppers**. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing and Activating Zones**.

NOTE: If the user fails to enter a correct user password 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user password. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

For more details on how to disarm & turn off the alarm by EKB2 keypad, please refer to chapter **3.2.5 Disarm & Turn off the Alarm by EKB2 Keypad**.

3.3.2 Arm by EKB3 Keypad in STAY Mode

EKB3

ATTENTION: The following procedure is described based on 4-partition mode operation on EKB3 keypad. If your alarm system installer has enabled 2-partition mode, the arming in Stay mode procedure using EKB3 keypad will be carried out identically to EKB3W wireless keypad. For more details on 2-partition mode, please refer to **3.3.3. Arm by EKB3W Keypad in Stay Mode**.

1. a) To Stay-arm a system partition that the keypad is assigned to, enter any out of 29 available 4-digit user codes or master code using the number keys:

Press the [STAY] key and enter user/master code:

STAY uuuu

Value: uuuu – 4-digit user or master code

Example: STAY2222

1. b) To Stay-arm a different system partition, switch the keypad partition by pressing and holding the [1]... [4] key for 3 seconds until you will hear 3 short beeps:

Switch keypad partition:

Hold the [1]... [4] key and release it after 3 short beeps:

Value: [1]... [4] key – partition number 1...4

After switching the keypad partition, press the [STAY] key and enter any out of 29 available 4-digit user codes or master code using the number keys:

Press the [STAY] key and enter user/master code:

STAY uuuu

Value: uuuu – 4-digit user or master code

Example: STAY2222

1. c) To Stay-arm multiple partitions simultaneously, press and hold the [0] key until you will hear 3 short beeps. Then press the [STAY] key enter any out of 29 available 4-digit user codes or master code using the number keys:

Hold the [0] key, release it after 3 short beeps, press [STAY] key and enter user/master code:

0 STAY uuuu

Value: uuuu – 4-digit user or master code.

Example: 0STAY2222

2. The keypad indicator **ARMED** and [1]... [4] key, corresponding the partition number that has been armed, will light ON.
3. In addition, the system will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.
4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it. For more details on how to view the violated zone / tamper number, please refer to **3.4 Alarm Indications and Viewing Violated Zones / Tamppers**. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing and Activating Zones**.

ATTENTION: Your alarm system installer must enable keypad partition switch feature before you can use it.

For more details on how to disarm and turn off the alarm by EKB3 keypad, please refer to chapter **3.2.7. Disarm and Turn off the Alarm by EKB3 Keypad**.

3.3.3 Arm by EKB3W Keypad in STAY Mode



1. a) To Stay-arm a system partition that the keypad is assigned to, enter any out of 29 available 4-digit user codes or master code using the number keys:

Press the [STAY] key and enter user/master code:

STAY uuuu

Value: uuuu – 4-digit user or master code

Example: STAY2222

1. b) To Stay-arm a different system partition, switch the keypad partition by pressing and holding the [1]... [2] key for 3 seconds until you will hear 3 short beeps:

Switch keypad partition:

Hold the [1]... [2] key and release it after 3 short beeps:

Value: [1]... [2] key – partition number 1... 2

After switching the keypad partition, press the [STAY] key and enter any out of 29 available 4-digit user codes or master code using the number keys:

Press the [STAY] key and enter user/master code:

STAY uuuu

Value: uuuu – 4-digit user or master code

Example: STAY2222

2. When the system is successfully armed, keypad indicator **ARMED** will light ON.
3. In addition, the system will reply with confirmation by SMS text message to the first preset user phone number (by default), assigned to the same partition as the user/master code.
4. When attempting to arm the system in case of violated zone / tamper presence, the system will not permit to arm it. For more details on how to view the violated zone / tamper number, please refer to **3.4 Alarm Indications and Viewing Violated Zones / Tampers**. For more details on how to arm the system in case of violated zones presence, please refer to **3.5 Bypassing and Activating Zones**.

ATTENTION: Your alarm system installer must enable keypad partition switch feature before you can use it.

NOTE: The user can control only the first two system partitions using EKB3W keypad.

For more details on how to disarm and turn off the alarm by EKB3W keypad, please refer to chapter **3.2.9. Disarm and Turn off the Alarm by EKB3W Keypad**.

3.4 Alarm Indications & Viewing Violated Zones / Tamppers



By default configuration, the system makes a phone call to User 1 in case of alarm. By answering the call, the user is able to listen on his/her mobile phone to what is happening in area surrounding ESIM364 unit. This feature is provided by a microphone (if any) connected to ESIM364.

The phone call is made to the next preset user (presumably to User 2) in a row in case the previous user was unreachable (was "out of radio coverage", provided "busy" signal or did not answer the call). This routine is continued until one of the preset users is reachable, but will not go in a circle i. e. return to User 1 if none of the users were reachable. In addition, the system will not make a phone call to the next preset user in a row if the previous user was reachable, but rejected the phone call. The phone calls will cease to be made to the user as soon as the system is disarmed.



Fig. No. 27

NOTE: Your alarm system installer may have configured the system to make the phone calls to the next available user even if the previous one has answered the call.

By, default configuration the system sends an SMS text message containing violated zone or tamper number in case of alarm. The SMS text message can also contain a text regarding wireless signal loss from a certain wireless device (if any) in case the tamper violation is caused due to wireless connection loss between ESIM364 and a wireless device.

This SMS text message is sent to User 1. The system sends the SMS text message to the next preset user (presumably to User 2) in a row only if the previous user was unreachable (the system did not receive a successful SMS text message delivery confirmation in 20 seconds from the recipient). This routine is continued until one of the preset users is reachable, but will not go in a circle i. e. return to User 1 if none of the users were reachable. The SMS text messages will cease to be sent to the user as soon as the system is disarmed.



Fig. No. 28

See also chapter **3.6 Viewing System Information**.

NOTE: Your alarm system installer may have configured the system to send the SMS text message to the next available user even if the previous one has received it.

The built-in EKB2 buzzer and ESIM364 buzzer (if any) provide short beeps continuously in case of alarm. In addition, the LCD screen back-light level will be boosted and the ! ! ! icon will be displayed in the home screen view of EKB2 keypad next to the violated partition name. The buzzer can be silenced by disarming the system using any method. Navigate through the following menu path using OK and arrow keys to view the violated zone or tamper number:

Menu path:

View violated zone: OK → uuuu → OK → VIOLATED ZONES → OK → ZONE 1... 76

View violated tamper: OK → uuuu → OK → VIOLATED TAMPERS → OK → TAMPER 1... 76

Value: uuuu – 4-digit user or master code.

The built-in EKB3/EKB3W buzzer emits short beeps continuously and ESIM364 buzzer (if any) emits a steady beep in case of alarm. In addition, the violated zone number is indicated by illuminated zone LED or flashing indicator **SYSTEM** (if the violated zone number is above 12). The violated tamper number is indicated by illuminated indicator **SYSTEM**. The buzzer can be silenced by disarming the system using any method.

When EKB3 keypad is operating in 4-partition mode, in case of violated zone/tamper [1]... [4] key will flash corresponding the alarmed partition number.

For more details on EKB3/EKB3W violated high-numbered zone & tamper number indication, please refer to chapter **3.10 Indication of System Faults**.



By default configuration, the siren/bell (if any) provides continuous alarm sound for 1 minute in case of alarm. The fire alarm is indicated by pulsating siren/bell alarm sound. The alarm sound can be silenced by disarming the system using any method.

3.5 Bypassing & Activating Zones

Arming the system is disabled while there's at least 1 violated zone. Bypassing allows to temporally deactivate a certain violated zone and arm the alarm system after-wards.



Enter valid user/master code and navigate through the following path using OK and arrow keys to bypass a violated zone (-s):

Menu path:

Bypass a zone: **OK → uuuu → OK → BYPASS → OK → BYPASS LIST 1... 3 → OK → ZONE 1... 76 → OK → BYPASS → OK**

Bypass all certain partition zones: **OK → uuuu → OK → BYPASS → OK → BYP VIOLATED ZONES → OK → [p] part-name → OK**

Value: *uuuu* – 4-digit user or master code.

Enter valid user/master code, navigate through the following path using OK and arrow keys to activate a bypassed zone:

Menu path:

Activate a bypassed zone: **OK → uuuu → OK → BYPASS → OK → BYPASS LIST 1... 3 → OK → ZONE 1... 76 → OK → UNBYPASS → OK**

Value: *uuuu* – 4-digit user or master code.

NOTE: Zones can only be bypassed and activated when the system is not armed.



Bypass a violated zone by entering a valid user/master code and entering the following combination using [BYP5], number and [#] keys:

Press the [BYP5] key, enter zone number and user/master code:

BYP5 nn uuuu #

Value: *nn* – zone number, range – [01... 76]; *uuuu* – 4-digit user or master code.

Example: *BYP5051111#*

NOTE: The zone will stay bypassed until the system is disarmed. Once the system is disarmed, the zone's current state will be indicated on the keypads.

ATTENTION: Bypassing a violated tamper is NOT allowed. Please, restore the tamper (for example: close sensor's enclosure) before arming the system

3.6 Viewing System Information



1. In order to find out the system's current information, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

ssss_INFO

Example: 1111_INFO

2. The system will reply to the user phone number that sent the SMS text message with the following up-to-date information:
 - System date & time.
 - System status: partition armed (ON)/disarmed (OFF).
 - GSM signal strength level.
 - Main power supply status.
 - Temperature of the area surrounding ESIM364 primary & secondary temperature sensors (if any).
 - State of zones (OK/alarm).

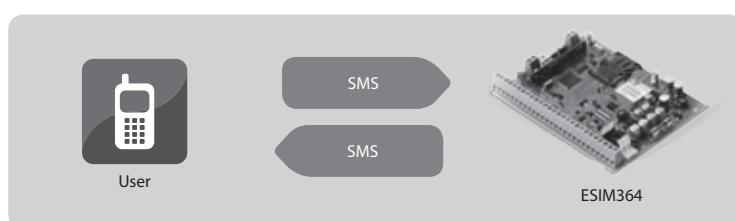


Fig. No. 29

See also [3.9 Managing Temperature Information](#).

3.7 Managing Periodical System Information



1. By default configuration, the SMS text message mentioned in chapter [3.6 Viewing System Information](#) is sent periodically to User 1 phone number at 11:00 daily.



Fig. No. 30

2. In order to set a different SMS sending frequency (in days) and time, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

ssss_INFO:ff:tt

Value: ff – frequency in days, range – [0... 10]; tt – time, range – [0... 23]

Example: 1111_INFO:2.15 (every 2nd day at 15:00)

NOTE: Unlike system information SMS text message upon request, periodical system information SMS text message does not include zone states, PGM output names and status.

3. In order to disable periodic SMS text message, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`SSSS_INFO:0.0`

Example: `1111_INFO:0.0`

4. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.



Fig. No. 31

3.8 Viewing Zone & PGM Output Information

SMS

1. In order to find out the current zone & PGM output information, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`SSSS_STATUS`

Example: `1111_STATUS`

2. The system will reply to the user phone number that sent the SMS text message with the following up-to-date information:

- System status: partition armed (ON)/disarmed (OFF).
- Status of zones & PGM outputs (ON/OFF).
- Zone alarm texts.
- PGM output names.



Fig. No. 32

3.9 Managing Temperature Information



1. The system supports up to 8 temperature sensors. If at least 1 or 2 (primary and/or secondary) temperature sensors are installed in your system, it can send an SMS text message containing temperature value in case the set lowest or highest temperature limit value is exceeded. This SMS text message is sent to User 1 only. By default configuration this SMS text message is disabled.



Fig. No. 33

2. In order to enable or set a different lowest, highest temperature limit value or specify a name for a determined primary or secondary temperature sensor, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_TEMPn:MIN:tm,MAX:tmx,NAME:temp-sens-name`

Value: *n* - primary or secondary temperature sensor number, range - [1... 8]; *tm* - lowest temperature limit boundary in °C, range - [-55... 125]; *tmx* - highest temperature limit boundary in °C, range - [-55... 125]; *temp-sens-name* - temperature sensor name, length - 4... 24 characters.

Example: `1111_TEMP2:MIN:-15,MAX:30,NAME:Garage`

3. In order to disable this SMS text message, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_TEMPn:MIN:0,MAX:0`

Value: *n* - primary or secondary temperature sensor number, range - [1... 8]

Example: `1111_TEMP1:MIN:0,MAX:0`

4. In order to find out, which temperature sensors are set as primary and secondary, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_TEMP?`

Example: `1111_TEMP?:`

5. In order to find out the current temperature of all temperature sensors, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_ITEMP?:`

Example: `1111_ITEMP?:`

6. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.

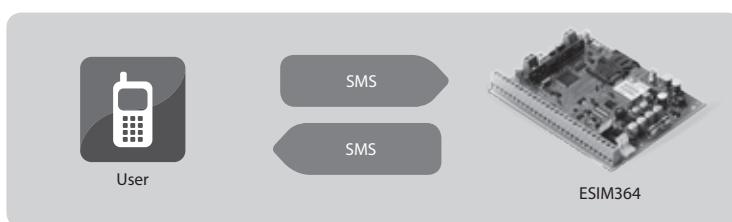


Fig. No. 34

See also chapter **3.6 Viewing System Information**

Enter valid user/master code and navigate through the following path using OK and arrow keys to view real-time temperature sensor values:

Menu path:

OK → uuuu → OK → TEMP SENSORS INFO → OK → 1... 8

Value: uuuu – 4-digit user or master code.

3.10 Indication of System Faults

 icon displayed in home screen view indicates presence of system faults. In order to view the currently present system faults, please enter a valid user/master code to access menu section **FAULTS**. The description on each system fault is provided in the table below.

Menu path:

OK → uuuu → OK → FAULTS → OK

Value: uuuu – 4-digit user or master code.

Name	Description
MAIN POWER LOSS	Main power supply is lost
LOW BATTERY	Low backup battery power - backup battery voltage is 10.5V or lower
BATTERY DEAD/MISS	Backup battery is not present or the battery voltage has run below 5V
BATTERY FAILED	Backup battery requires replacement - backup battery resistance is 2Ω or higher
SIREN FAILED	Siren is disconnected/broken
VIOLATED TAMPER	One or more tampers are violated
DATE/TIME NOT SET	Date/time not set
GSM CONNECT FAILED	GSM connection is lost
GSM/GPRS ANTENNA FAILED	GSM/GPRS antenna is disconnected/broken
KEYPAD LOST	Keypad is disconnected/broken

Yellow LED **SYSTEM** indicates system faults. **SYSTEM** LED indications are mentioned in the table below.

SYSTEM LED	Description
Illuminated continuously	One or more zones or tampers are violated; other system faults
Flashing	One or more high-numbered zones are violated

In order to find out more on the particular system problem please , enter command A. After this procedure the system will activate red zone LEDs for 15 seconds. The description on each LED indication is mentioned in the table below.

Zone LED	Description
1	Main power supply is lost
2	Low backup battery power - backup battery voltage is 10.5V or lower
3	Backup battery is not present or the battery voltage has run below 5V
4	Backup battery requires replacement - backup battery resistance is 2Ω or higher
5	Siren is disconnected/broken
7	One or more tampers are violated
8	Date/time not set
9	One or more high-numbered zones (Z13 - Z76) are violated
10	GSM/GPRS connection is lost
11	GSM antenna is disconnected/broken
12	Wireless antenna is disconnected/broken

In order to find out which particular high-numbered zone is violated please , enter command B.

In order to find out which particular tamper is violated please , enter command C.

A. System fault indication - enter command:

[CODE#]

B. Violated high zone indication – enter command:

[CODE1]

C. Violated tamper indication – enter command:

[CODE2]

The number of violated high-numbered zone or tamper can be calculated using the table below according to the formula: number from zone LED section B + number from zone LED section A.

Example: LED #3 from section A is flashing and LED #8 from section B is illuminated continuously. According to the table below LED #8 is equal to number 18, therefore $18 + 3 = 21$.

Result: Violated high-numbered zone or tamper number is 21.

Zone LED section - A (flashing)	Zone LED section - B (illuminated continuously)
Zone LED 1 = 1	Zone LED 7 = 12
Zone LED 2 = 2	Zone LED 8 = 18
Zone LED 3 = 3	Zone LED 9 = 24
Zone LED 4 = 4	Zone LED 10 = 30
Zone LED 5 = 5	Zone LED 11 = 36
Zone LED 6 = 6	Zone LED 12 = 42

3.11 Controlling Electrical Appliances

Your system features 4 or more PGM outputs intended for connection and control of various electrical appliances. This provides a possibility to control garage gates, turn on and off your house heating, lighting, cooling system, reset smoke sensors to restored state etc. The PGM outputs must be configured by your installer before using them.



1. In order to turn ON a specified PGM output, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_Coo:ON` or `ssss_out-name:ON`

Value: *oo* – PGM output number, range – [1... 76]; *out-name* – PGM output name.

Example: `1111_Pump:ON`

2. In order to turn OFF a specified PGM output, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_Coo:OFF` or `ssss_out-name:OFF`

Value: *oo* – PGM output number, range – [1... 76]; *out-name* – PGM output name.

Example: `1111_C2:OFF`

3. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.



3.12 Turning ON/OFF the Electrical Appliances for a Determined Time Period

SMS

1. In order to instantly turn ON a specified PGM output and keep it in this state for a determined time period, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_Coo:ON:hr:mn:sc` or `ssss_out-name:ON:hr:mn:sc`

Value: `oo` – PGM output number, range – [1... 76]; `hr` – hours, range – [00... 23], `mn` – minutes, range – [00... 59]; `sc` – seconds, range – [00... 59]; `out-name` – PGM output name.

Example: `1111_Pump:ON:00:00:25`

2. In order to instantly turn OFF a specified PGM output and keep it in this state for a determined time period, send the following SMS text message to the system's phone number from any out of 10 preset user phone numbers:

SMS text message content:

`ssss_Coo:OFF:hr:mn:sc` or `ssss_out-name:OFF:hr:mn:sc`

Value: `oo` – PGM output number, range – [1... 76]; `hr` – hours, range – [00... 23], `mn` – minutes, range – [00... 59]; `sc` – seconds, range – [00... 59]; `out-name` – PGM output name.

Example: `1111_C3:OFF:13:25:56`

3. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.

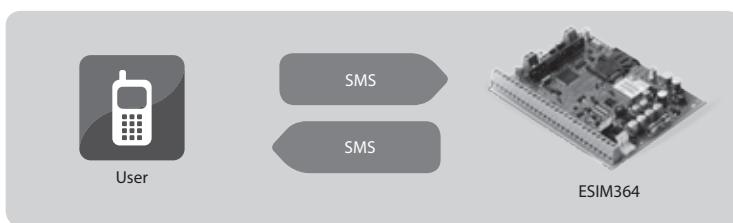


Fig. No. 36

NOTE: PGM output can be turned ON for a determined time period only when it is in OFF state.

NOTE: PGM output can be turned OFF for a determined time period only when it is in ON state.

3.13 Viewing Event and Alarm Logs

The event log allows to chronologically register up to 500 timestamped records regarding the following system events:

- System start.
- System arming/disarming.
- Zone violated/restored.
- Tamper violated/restored.
- Zone bypassing.
- Wireless device management.
- Temperature deviation by MIN and MAX boundaries.
- System faults.

The event log is of **LIFO (last in, first out)** type that allows the system to automatically replace the oldest records with the latest ones.

Enter master code and navigate through the following menu path using OK and arrow keys to view the event log:

Menu path:

OK → uuuu → OK → VIEW EVENT LOG → OK

Value: uuuu - 4-digit master code.

The alarm log provides a list of last 16 alarm events generated after last arming period. The alarm log can be viewed via EKB2 and includes only the alarms of the partition that the user/master code is assigned to. Each alarm record includes alarm type, partition number and zone number. When highlighted, the date and time of the alarm occurrence can be viewed at the bottom of EKB2 screen. In case of alarm,  icon will appear in home screen view of EKB2. The alarm log auto-clears when the next system arming follows or after viewing it via the keypad.

Enter user or master code and navigate through the following menu path using OK and arrow keys to view/clear the alarm log:

Menu path:

OK → uuuu → OK → ALARM LOG → OK

Value: uuuu - 4-digit user or master code.

4. IF THE ALARM SYSTEM IS CONNECTED TO MONITORING STATION

The following system features may be disabled by your alarm system installer if the system is connected to a monitoring station:

- Confirmation by SMS text message when arming, disarming & turning off the alarm by phone call, SMS text message, EKB2/EKB3/EKB3W keypad, iButton® key, EWK1/EWK2 - wireless key-fob..
- Alarm indication by phone call.
- Alarm indication by SMS text message.
- Violated zone/tamper name indication by SMS text message.
- Temperature indication by SMS text message.
- Periodical system information by SMS text message.
- Main power loss/restore indication by SMS text message.
- Any other SMS text message generated by the system.

NOTE: For complete system configuration and control, please refer to ESIM364 installation manual located at www.eldes.lt/en/download

Made in Lithuania.
www.eldes.lt

iButton is a registered trademark of Maxim Integrated Products, Inc.